Introdução ao Teste de Invasão e Ética Hacker

"Se você conhece o inimigo e conhece a si mesmo, não precisa temer o resultado de cem batalhas. Se você se conhece mas não conhece o inimigo, para cada vitória ganha sofrerá também uma derrota. Se você não conhece nem o inimigo nem a si mesmo, perderá todas as batalhas." - *Sun Tzu*

Objetivos

- Fornecer ao aluno uma visão geral sobre testes de invasão
- Entender a anatomia e os tipos diferentes de ataques
- Conhecer as fases de um teste de invasão
- Conhecer as metodologias e os apectos legais

OYS ACADEMY

Visão geral sobre o Pentest

- O Teste de Invasão é um processo de análise detalhada do nível de segurança de um sistema ou rede usando a perspectiva de um infrator.

- O objetivo principal é simular de forma controlada um ataque real que normalmente é executado por criminosos.

OYS ACADEMY

Tipos de Pentest

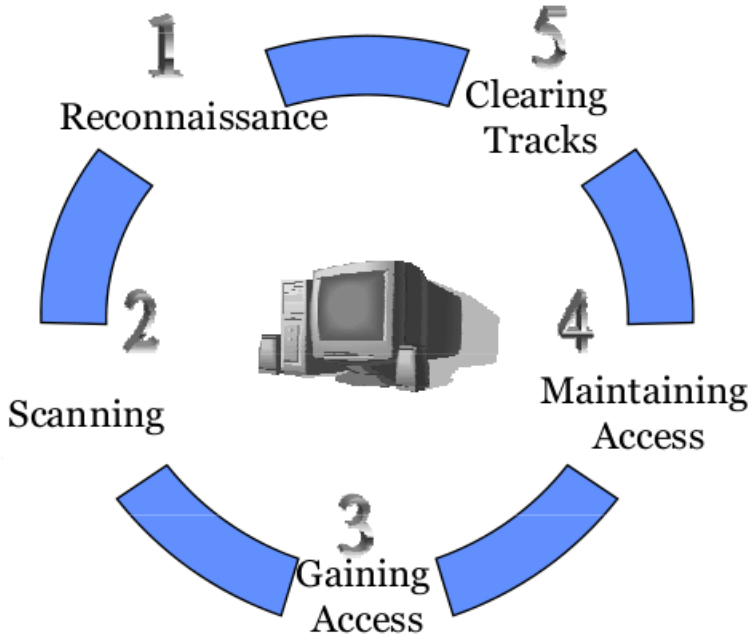
- Blind
- Double blind
- Gray Box
- Double Gray Box
- Tandem
- Reversal

OYS ACADEMY

As fases de um ataque

- Os procedimentos realizados por um profissional de teste de intrusão é similar aos realizados pelos crackers, diferindo na intenção do ataque.

- Levantamento de informações
- Varredura
- Ganhar acesso
- Manter acesso
- Apagar rastros



OYS ACADEMY

Categorias de ataques

- **Server Side Attack**

•Foca na tentativa de explorar serviços que estão em execução em um determinado dispositivo

•Não precisa de interação do usuário

- **Client Side Attack**

•Foca na tentativa de explorar aplicações que são executadas no computador e que normalmente precisam de uma interação da pessoa para que o ataque seja executado

OYS ACADEMY

Metodologias existentes

- OSSTMM
- OWASP Testing Guide
- NIST SP800-115 e SP800-42
- ISSAF
- PenTest Frameworks

OYS ACADEMY

Como conduzir um teste de invasão

- **Passo 1:** Converse com seu cliente sobre as necessidades do teste;
- **Passo 2:** Prepare o contrato de serviço e peça ao cliente para assiná-los;
- **Passo 3:** Prepare um time de profissionais e agende o teste;
- **Passo 4:** Realize o teste;
- **Passo 5:** Analise os resultados e prepare um relatório;
- **Passo 6:** Entregue o relatório ao cliente.

Aspectos Legais

- Um dos aspectos importantes de se manter sempre em mente é o seguinte:
  - **Teste de Invasão sem permissão é crime!**
- Atentar para os tipos de ataques que serão testados, para evitar causar situações que gerem algum tipo de comprometimento nos serviços do cliente.
- Criar imagens dos servidores críticos que serão testados e realizar os testes em sandbox, com máquinas virtuais.
- Esses aspectos são importantes, para que não ocorram qualquer anomalia em qualquer um dos pilares da segurança da informação, e o cliente sofra alguma perda de informações ou prejuízos financeiros.

"Não prestamos muita atenção à segurança da informação. Esperamos que nossos concorrentes roubem nossas idéias e tornem-se tão fracassados como nós."

OYS ACADEMY

Escrita de Relatório

OYS ACADEMY

Objetivos

- Um relatório é um conjunto de informações, utilizado para reportar resultados parciais ou totais de uma determinada atividade, experimento, projeto, ação, pesquisa, ou outro evento, esteja finalizado ou ainda em andamento.
- *Fonte: wikipedia.org*

OYS ACADEMY

O que deve conter no relatório?

- Capa
- Índice
- Classificação do nível de confidencialidade do documento
- Sumário executivo
- Definição do escopo
- Definição dos vetores de ataque
  - Mapeamento da rede e definição dos alvos
- Ataques realizados
  - Ferramentas utilizadas
  - Exploits executados
  - Comandos utilizados
  - Resultados recebidos
  - Classifição das vulnerabilidades por nível de facilidade de exploração, popularidade, impacto, e tirando a média desses 3, informando o risco.
- Solução, onde informa possíveis soluções para as vulnerabilidades encontradas

OYS ACADEMY